T-O-P S-E-C-R-E-T

September 30, 1944.

MEMORANDUM

TO: The Minister

FROM: Mr. Higgs

I attended a secret meeting yesterday afternoon, September 29, at 5 p.m. with Col. Hallamaa, Chief of Finnish Military Intelligence. The meeting was arranged by Mr. Tikander and Prof. Cole, both of whom were also present, and who had had previous conversations with Col. Hallamaa. In this connection reference is made to Mr. Tikander's memorandum of September 26 to the Minister regarding information obtained from Col. Hallamaa.

Col. Hallamaa was most pleasant and seemed to be entirely frank and open regarding the matters discussed. His attitude was one of quiet confidence and restrained pride, but with no suggestion of boasting. His English was so hesitating that the conversation with him was conducted in Finnish with Mr. Tikander translating. Col. Hallamaa made the following statements regarding the activities and findings of his organization with respect to American and other codes:

1. Only some ten or twelve expert cryptologists worked on our codes, one of whom, however, was probably his best man. Col. Hallamaa denied that he had any cryptographic abilities, saying he was merely administrative head of the unit.

2. The Finns had broken our Gray, Brown, and strip codes, and "others" whose names he could not recall, but which undoubtedly were A, B, and C, for later in the conversation he referred to our transposition codes which he said had been broken. He used the English names for Gray, Brown, and strip codes and spoke of our "inter-communicating strip". He was uncertain exactly how many of our strip series had been "compromised"--he used that word, saying he had observed that we used the term ourselves in our messages--and that he would have to ask his assistants.

He

DECLASSIFIED
E.O. 12356
NND 11698
by SDT Date 4/9/02

STATE DEPT. DECLASSIFICATION REVIEW
☐ Retain classification Changed classify to _____
☒ Declassify with concurrence of _____
other _____
Reviewer WM Lindy Date 7-2-99

He gave the impression, however, that the only difficulty encountered in decoding our strip ciphers was one of personnel shortage, that is, that during certain periods available experts were shifted to other codes of more urgent interest to Finland than ours.

Col. Hallamaa, replying to a question, said that so far as he knew no other country was using the strip system, except, he said laughingly, Finland after the Finns learned of it from us. He said his expert on our strip cipher could give a "four hour lecture" on the theories and technical capabilities of the strip.

3. He, himself, did not think there was much to choose between when comparing the security features of the strip and the double transposition systems.

4. They had been greatly aided in their work on breaking our strips by carelessness on our part in the preparation of our messages, and by the volume of the messages obtained. For instance, he said we were constantly putting information in ciphers they had already broken regarding messages in new ciphers, after which they could "crack" the new ones. Also some missions would repeat to other missions in already-broken ciphers verbatim messages received by the former in new ciphers and this enabled the Finns to break the new ones immediately. A careless few lines in clear also had proved most helpful on occasion.

5. Regarding the strip system generally he considered it as secure as any other, with the exception of the "pad" (or "block" as he called it). He said the latter "could not be broken" (Dave Salmon told me the same thing once, though he did not say why we didn't use it).

6. Replying to my request for information regarding the contents of the messages from our Legation in Bern to the Department, Col. Hallamaa said the great bulk of them were intelligence messages dealing with conditions in Germany, France, Italy, and the Balkans. He spoke in complimentary terms about

"Harrison's"

"Harrison's" information-gathering abilities.

I encouraged him to continue discussing the Bern messages, hoping he would eventually describe their one characteristic not common to messages from other missions. Eventually he did so, and without any guidance whatsoever from me: He said that when the first began reading the Bern messages they named the sources of the information; then the Legation stopped giving the names in the messages but referred to previous messages therefor; and finally they gave informants numbers with the result that messages read "according to X241...". This is an accurate account of the Bern messages, according to my personal knowledge of them.

7. He was rather vague as to how recently they were decoding our messages. He did say, however, that they had decoded Steinhardt's messages from Ankara regarding the recent Rumanian armistice negotiations. His general confidence in their ability to decode any of our messages anytime they wanted to, suggests very strongly that they do just that and that the limits on their achievements from time to time arise from personnel inadequacies rather than the nature of our codes.

8. He showed knowledge of the fact that some American missions are using machine codes, but did not say these had been broken though he seemed confident it could be done whenever the Finns so desired.

9. He mentioned that the Finns had also broken the codes of Brazil, Bulgaria, Turkey, Spain, and the Vatican. He would not admit they had broken the German codes though he did say the Germans have a machine code which he said was called "Enigma", of which there was a diplomatic and a military model.

Most of their efforts, he pointed out, were naturally exerted on Soviet codes, of which he claimed they had broken over a thousand. He exhibited convincing specimens of their work on Soviet codes.

10. Further regarding our Helsinki messages,

Col.

Col. Hallamaa recalled with amusement a telegram McClintock had sent to the Department reporting that Marshal Mannerheim had told him "the Germans" had broken our codes. The Colonel implied that he considered this action on the part of the Marshal was not only very friendly but also sporting.

Col. Hallamaa said that they always knew before McClintock arrived at the Foreign Office what he was coming to talk about. He did not think his organization's work was passed on to the Foreign Office, however, as the Marshal had said the Foreign Office was too talkative. I asked him if his organization received copies of aide memoire, etc., left by our mission at the Foreign Office, and if so to what extent these documents assisted his work. He replied that they always received copies of such documents, but that they were not especially helpful for his purposes. (When asking this question I had in mind the possibility that faulty or careless paraphrasing might account for some of the compromises of our codes.

I also asked Col. Hallamaa if they had placed microphones in our Legation. He laughed and said no. He said they had been quite amused at McClintock's messages recounting the searches made by Varga.

11. Col. Hallamaa was vague about the extent to which messages from the Stockholm Legation had been worked on and broken. The implication was clear, however, that, as with American messages in general, he was completely confident that they could break these if they really wanted to.

12. He denied knowledge of German activity with respect to American codes and remarked that "Black Chambers" of various nations seldom confided their secrets to each other. He did say, however, that the Germans had several times requested the code texts of our Helsinki Legation messages.

13. All code texts of our messages falling into the hands of the Finns were obtained by radio interception.

14. Col. Hallamaa's leading cryptographic experts

are

are now residing secretly in Sweden. He is currently trying to work out some scheme for their disposition, and while he did not say so I think he would be glad to have us take them over.

* * * * *

I should like to record in connection with this conversation that the Legation representatives present were most careful at all times to say nothing regarding any similar activities on the part of the United States, or to give away any information regarding our codes which Col. Hallaman did not demonstrate beyond all doubt he already had.

L. R. H.

LHH:VE